Design of Secure Key Establishment Protocols: Successes, Failures and Prospects

Colin Boyd*

Information Security Research Centre
Queensland University of Technology
Brisbane Q4001, Australia
boyd@isrc.qut.edu.au

Abstract. Key establishment protocols form one of the most basic types of cryptographic protocols and have been studied intensively for over 20 years. The current status of design and analysis methods is reviewed with particular reference to formal appoaches. Likely future trends and open issues are also discussed.

1 Introduction

Key establishment is a foundational element for secure communications. It concerns how to set up a new key (a *session key*) to protect communications during a subsequent session. In terms of modern cryptography it is a venerable problem that has been widely studied from almost every conceivable angle. One may ask how hard it can be to consider all ways of setting up a session key. Yet the evidence is that this study has not yet been exhaustive. One reason for this is that new requirements have become evident over time that were not previously recognised. Another reason is that there is no well-defined method to explore the space of possible secure protocols. Even until today most systematic or formal techniques allow only protocol analysis and not design of protocols to meet specific requirements. The purposes of this paper are:

- to explore current techniques to ensure the security of key establishment protocols, particularly those with some formal basis;
- to consider to what extent these methods can be used to systematically design new protocols;
- to summarise (and speculate on) prospects for the future of these methods.

In the rest of this introduction some background information is provided on protocol types and potential security requirements. Section 2 looks at informal design principles for key establishment. Sections 3 and 4 are devoted to the two main formal approaches to protocol analysis: the formal methods approach which comes from the computer security research community, and the computational

* Research funded by Australian Research Council under Discovery Project DP0345775.

approach which comes from the cryptography research community. Section 5 discusses current trends and prospects for combining the benefits of both these approaches.

1.1 Key agreement and key transport

A common way of classifying key establishment is to consider protocols which provide either *key agreement* or *key transport*. Key agreement protocols require input to the session key from both parties in a two-party protocol, or more generally from more than one party in a multi-party protocol. In a key transport protocol one party (often a trusted third party) chooses the key and forwards it to the other parties.

It is often stated that key agreement is preferable to key transport. Reasons given are that key agreement is 'fairer' since no party is able to fix the key value. However, this property does not correspond to any standard security property and most models do not in any case take account of malicious insiders. Since any party is free to give away the session key at will, what may be the benefit of making the key some fixed value? In addition, it is often suggested that using pseudo-random input from more than one party serves to increase the randomness of the final key. This may or may not be useful depending on how the values are combined. In particular, suppose that two parties A and B provide values g^x and g^y in the classic Diffie-Hellman key agreement protocol. If the random number generator of A is very weak then it may be easy for an adversary to obtain x and hence the shared key g^{xy}, no matter how strong is the random number generator of B[1].

1.2 Adding Requirements

One reason that key establishment continues to be a challenging problem is the addition of new properties that are desired in certain situations. These include ways of strengthening the security properties such as the following.

Forward secrecy is the property that compromise of long-term keys should not compromise session keys that were previously accepted. Forward secrecy is increasingly regarded as a very desirable property. It seems to be achievable only through the use of ephemeral public keys, such as in Diffie-Hellman key exchange. (Although it is not widely recognised, ephemeral keys from any public key encryption scheme can be used to provide forward secrecy, including RSA as noted by Wiener [Wie98].)

Resistance to key compromise impersonation is a less widely discussed property that is related to forward secrecy in that it concerns what may happen after long-term keys are compromised. It demands that the adversary who has obtained the long-term key of entity A is unable to masquerade as other principals to A.

[1] This observation was made to me by Carsten Rudolph.

Anonymity of principals was often neglected in the past, but with the prevalence of communications on public (including wireless) networks it is more widely recognised as an issue. For example, the Internet Key Exchange (IKE) protocol [HC98] explicitly addresses this requirement, although its provision is not so robust as may have been initially expected [PK00].

Resistance to denial of service is a pressing practical need for protocols, particularly those run on open networks. This is another property that was considered in the design of IKE, although there has been much controversy over the resulting solution [PK00].

As well as the above extra security features that can be relevant to any security architecture, some protocols have extra fundamental assumptions about the way that the network is set up and the security infrastructure in place.

Group key establishment protocols have become very popular in the recent literature in line with the increase in collaborative communications applications. There are many possible types of architecture. One of the most challenging is the ad-hoc network where the security infrastructure may be minimal.

Low-power principals are as prevalent as ever, due to the inexorable miniaturisation of devices. The most common example has been the mobile telephone, and there are many protocols designed specifically for its use. New lightweight technologies, such as RFID tags, open up new challenges.

Password-based protocols were first introduced around 15 years ago. These protocols assume that shared keys have only a small amount of entropy, and must therefore be robust against off-line guessing attacks in which the adversary attempts to eliminate potential passwords using public information. Recently such protocols have attracted extensive interest, and standards in both IEEE [IEE04] and ISO are in preparation.

Identity-based protocols have been around for about 20 years but recent techniques based on elliptic curve pairings have resulted in an explosion of interest in this area. These protocols allow users to establish keys without the use of an on-line server or a public key infrastructure. There is likely to be continuing interest in this area and to date few key establishment protocols using the new techniques come with a proof of security.

Notice that most combinations of the above requirements or scenarios are possible, although some are in conflict with others. For example, protocols providing forward secrecy are typically more computationally expensive than those that do not. Therefore protocols designed for low-power principals often sacrifice forward secrecy for benefits in efficiency.

2 Design Principles

In 1994 Abadi and Needham gathered together the experience of many years and produced a set of 11 rules of thumb to be used as principles for designers

of cryptographic protocols [AN94]. The following year Anderson and Needham [AN95] added a set of "robustness principles" aimed specifically at protocols in the public-key setting.

The Abadi-Needham principles can be viewed as common sense rules that can be applied in an informal protocol design process. Undoubtedly the informal design of simple protocols has benefited from wide knowledge of these rules. However, it is interesting to note that at least two, and arguably four, of the rules are about clearly defining various aspects of the protocol specification. In addition two of the seven principles of Anderson-Needham fall into this category. In other words these informal rules can be regarded as promoting the use of formality in protocol analysis.

One of the principles of Abadi and Needham can be roughly paraphrased as 'sign-before-encrypting'. In other words, when it is required to provide both authentication and confidentiality to some data, the plaintext should be signed and the result should then be encrypted. The idea behind this rule is intuitively clear: a signature of a ciphertext does not imply that the signer ever knew the plaintext. Indeed, there are several protocol attacks in which a signature on a ciphertext is removed by the adversary and replaced with a new signature. It is therefore somewhat surprising to find that many successful protocols, even those with proofs of security, ignore this rule. Paradoxically, much later analysis of the security of combining authenticity and encryption [ADR02] indicates that signing before encryption tends to give security properties no stronger than applying these operations the other way around.

3 Formal Specifications

Formal methods of specification and analysis, usually supported by software tools, have been used to analyse key establishment protocols for over 15 years. The typical analysis model uses a paradigm introduced by Dolev and Yao [DY83] in which cryptography is treated as a 'black-box' operation. This means that the adversary is able to encrypt and decrypt with any keys that it knows, but without the necessary keys will be unable to do anything with a ciphertext. Numerous formalisms and tools have been used over the years. Generally the tools search the available state space and try to establish whether insecure states can be reached. Various methods have been used to enhance the searching process. Meadows [Mea03] provides a detailed introduction to the history and progress of this research area.

3.1 Successes

There are some well-documented cases of new and unexpected attacks on protocols that have been found by machine analysis. The most celebrated is Lowe's discovery [Low96] of a flaw in the public-key protocol of Needham and Schroeder [NS78] which was found in 1996, close to 20 years after the protocol's first publication. The attack is surprisingly simple and once seen looks very obvious and not at all something beyond the capacity of a systematic search by hand.

In addition to finding flaws many protocols have been certified as free from flaws using analysis of formal specifications. Model checkers can be used to check protocols quickly and in an automated fashion. As one recent example, Basin *et al.* [BMV03] report that their 'on-the-fly model checker' (OFMC) was able to check all 36 protocols from the well known Clark–Jacob library [CJ97] in less than one minute of processing time.

3.2 Failures

A major limitation of models based on Dolev-Yao is that there is no succinct representation of the security property attained by a protocol that passes the analysis. What we know is that there is no adversary that can gain the stated secrets using the operations in the way specified. But that does not mean that there are not other strategies for the adversary that may be successful. Backes and Schunter [BS04] describe an example in which a mobile agent security protocol was formally verified to be secure with an automated theorem prover and yet it turned out to be vulnerable to a simple attack. Backes and Schunter point out that the reason for this failure was the omission of a critical action which the adversary should be allowed. Once the attack is discovered it is easy to include this action into the adversary's repertoire. A possible conclusion is that you need to already know about the potential types of attack in order to find them using the this type of model. It is perhaps harsh to regard this example as a criticism of formal methods, since protocols of the type used in this case have not yet been modelled at all using the computational models described below.

A second, and more obvious, limitation of the Dolev-Yao approach is that the cryptographic properties are not modelled faithfully. One aspect of this is that partial information leakage and probabilistic behaviour is typically ignored. A related, practically significant, issue is that different definitions of confidentiality are not distinguished. In the cryptographic community there are several different standard definitions of confidentiality including indistinguishability and non-malleability, and protection against either known plaintext or chosen plaintext attacks. Generally algorithms with stronger properties are less efficient and require stronger assumptions, so it is a good principle to use the weakest assumptions possible regarding the cryptographic algorithm required. Having found the attack on Needham-Schroeder protocol mentioned in Section 3.1, Lowe proposed an improvement which showed no weaknesses using his technique. However, neither in the original definition, nor in his improved protocol, is there a specification of the encryption algorithm to be used in terms of the standard definitions. It is not hard to see that some form of non-malleability must be provided and Lowe does point out that the adversary must not be able to alter an encrypted message. Recently Warinschi [War03] has given a computational proof assuming that the encryption algorithm has a strong security property.

3.3 Prospects

There is no doubt that research using formal methods for protocol analysis is as active as it ever has been. The plethora of tools and formalisms that were applied during the 1990s revealed new insights but it is now widely recognised that advances are required to 'go beyond Dolev-Yao' by incorporating new properties and exploring new requirements. Meadows [Mea03] provides a comprehensive review of future trends. Some of the main directions that she mentions are coverage of denial of service, anonymity, and more cryptographic properties. Meadows remarks on the trend to analyse real-world protocols, particularly those in standards. Backes and Schunter [BS04] provide a "cryptographers' wish-list" of Dolev-Yao extensions which overlaps with the issues identified by Meadows.

None of the current tools can really be used as design methods except in the sense that there are some (relatively) automatic and quick analysis tools that can be used to provide quick feedback on prototype designs. Meadows [Mea03] remarks that a possible direction towards using animation to help designers does not seem to be developing. There has been some work using tools to search for good protocols in the set of all possible protocols [CJ02]. So far it is not demonstrated that these can find useful new protocols with specified properties.

4 Provable Security

The cryptographic research community has evolved in the past 10-15 years to embrace formal foundations based on computational definitions and reductionist proofs. Acceptance of the approach is now widespread although there remain controversies [KM04], particularly when the so-called *random oracle model* is adopted. Initially the computational definitions concentrated on basic algorithms such as encryption and signature schemes. Key establishment was first considered in 1993 and interest has blossomed since the late 1990s.

4.1 Bellare–Rogaway Model

Bellare and Rogaway [BR93] initiated the computational study of key establishment in 1993. Their first paper covered only a two-party protocol between two users who already share a long-term key. Two years later [BR95] this was extended to a three-party protocol including a trusted server in the style of Needham and Schroeder's shared key protocol.

In models of this type the adversary runs the protocol in the sense that it controls which parties send and receive messages. To do this the adversary issues a Send query. The adversary has the ability to fabricate any messages that it can compute and use these as messages. In addition the adversary can obtain any session key that has been accepted by issuing a Reveal query regarding any party instance. The adversary can also issue a Corrupt query regarding any party and obtain and modify its long terms keys. These capabilities model the ability of a protocol adversary to mount replay attacks and insider attacks. The adversary

eventually issues a Test query for a session that has not been opened by a Reveal or Corrupt query. The adversary's goal is to reliably distinguish between the key accepted in the test session and a random key. This is a strong definition of security but one which corresponds to the prevailing definition of security for confidentiality in encryption algorithms. The adversary is restricted only in that it has bounded computational power; specifically it must be a probabilistic polynomial time algorithm.

Successes By now there have been quite a few protocols proven secure in the Bellare–Rogaway model, or close variants. These include public key transport protocols, key agreement protocols, password-based protocols, multi-party key agreement and identity-based protocols. One may argue that the number of proven secure protocols is nevertheless quite small in comparison with the range of key establishment protocols currently known. Proving a protocol in this model is no small undertaking and most of the relevant papers contain proofs for only one or two protocols and require several pages of human-generated mathematical reasoning.

Failures One criticism of the provable security approach in general is inaccessibility of the proofs. This leads in turn to a lack of wide scrutiny of the proofs [KM04]. There have been well-publicised failures in computational proofs for encryption. Proofs have also been claimed for key establishment protocols that were subsequently shown to be insecure. A protocol designed for low-power devices by Jakobsson and Pointcheval was initially published in a pre-proceedings version which was shown by Wong and Chan to be vulnerable to a simple masquerading attack [WC01]. Subsequently the protocol was fixed with a small change.

Another issue is whether protocols proven secure can be implemented in a way that they can be practically used. An important part of the security definition requires the identification of the partner of any principal in a protocol run. This is because the adversary must be forbidden from obtaining a session key in a trivial way by revealing the key from a partner who has accepted. In different versions of the Bellare–Rogaway model partnering has been defined in different ways. The most recent versions [BPR00] used the natural idea of *session identifiers*. This way of defining partners is not only intuitively clear (thus making the proofs more transparent) but also gives a practical way for entities to identify which key to use (for example on a particular communications socket). It turns out that the 1995 protocol proven secure by Bellare and Rogaway [BR95] has no reasonable way to define session identifiers. This means that although the protocol is secure it does not seem very useful. Choo *et al.* [CBHM04b] showed how a simple change to the protocol allows a natural session identifier to be defined, which can also be used in the protocol proof.

Prospects Over the ten years and more since Bellare and Rogaway introduced their model there have been significant extensions. This has usually taken the

form of new capabilities made available to the adversary to fit new requirements. For example, password-based protocols are accommodated by restricting the adversary's ability to use Send queries since each such query may be used to test a single password. Instead a new Execute query allows the adversary to observe protocol runs without trying a password guess.

Although the basic model is now firmly established, it seems likely that new variations will continue to evolve to cater for new requirements. Very recently Abdalla *et al.* [AFP04] proposed a variation in the adversary capability which allows multiple Test queries which consistently respond with the real key or a random one. Looking back at some of the additional requirements mentioned in Section 1.2 we can see that there is potential for some new additions to the model. Forward secrecy is already catered for through use of the Corrupt query, but key compromise impersonation and anonymity do not yet seem to have been modelled. These two seem to be quite achievable in this type of model, but denial of service is an area that seems to fall outside the scope of the usual computational models.

It is clear that analysis in the Bellare–Rogaway model does not provide an efficient way to design a new protocol. Varying an existing protocol is very likely to break an existing proof and there seems no useful way to guess whether a proof is possible for a new protocol.

4.2 Modular proofs

In 1998, Bellare, Canetti and Krawczyk [BCK98] suggested a method for modular proofs of key establishment protocols. The basic idea is to first prove the protocol secure in an ideal world where messages are automatically authenticated. This ideal world is called the *authenticated links model* or simply the AM. This roughly corresponds to the situation where the adversary is passive, so unable to alter or fabricate messages (although the adversary is able to effectively delete messages). Having proved the protocol secure in the ideal world it can then be transformed into a protocol in a more realistic model in which the adversary does have the ability to fabricate messages — indeed the capabilities of the adversary are basically the same as those in the Bellare–Rogaway model.

The initial model of Bellare *et al.* [BCK98] used a security definition based on emulation between protocols in the two worlds. Later it was found that this definition is too strict to be useful and so, in 2001, Canetti and Krawczyk published a revised model [CK01] with a definition of security based on indistinguishability, similar to that of Bellare and Rogaway. Another significant benefit in the new model is that it is proven that the agreed session key can be used safely to provide secure channels, a property absent from the Bellare–Rogaway model.

Successes The modular approach uses two types of components: the simplified protocols in the ideal world (called AM protocols) and the compilers to transform protocols into the real world (called authenticators). One of the significant benefits of the modular approach is the ability to *reuse* any AM protocol with

any authenticator. Consequently, when one new component is proven secure, a whole set of new protocols results whose members are all automatically proven secure. As the number of components increases the multiplying effect of adding other components becomes more significant.

The separation of concerns between session key confidentiality and authentication also allows a much easier way to select components suitable for different applications. In other words, we may regard the modular approach as a step towards a design method for provably secure key establishment protocols. The initial papers of Bellare *et al.* provided only a couple of examples of authenticators and AM protocols. Subsequently a number of additional examples have been provided including: a password-based authenticator [HTN+03] an authenticator based on static secrets (including identity-based secrets) [BMP04]; an AM protocol using ElGamal-type encryption [TBN03]; and an AM protocol mixing symmetric and asymmetric encryption [TVBN04].

Failures A significant limitation of the modular approach is that it may not be possible to reach all desirable protocols by decomposing into AM protocols and authenticators. In particular, despite the existence of password-based authenticator when the server has a public key [HTN+03], password-based protocols that do not use server-public keys do not seem to allow any useful separate authenticator. This is not a limitation of the computational approach in general, since such protocols have been proven secure in the Bellare–Rogaway model [Mac02,EBP04].

A second limitation concerns the 'post-processing' of proven-secure protocols. In order to derive efficient protocols using the modular approach, it is necessary to perform some optimisation steps, particularly in the case where the AM protocol has more the one message. Currently this process is informal, so any resulting protocol strictly no longer has a security proof.

Prospects It seems likely that more protocol components can be added to the library of existing proven secure components. This will lead to a significant number of additional protocols due to the multiplying effect mentioned above. Another likely development is the formalisation of the optimisation steps in order to make the whole process of obtaining an efficient protocol fully formal.

One direction that has not been explored yet in the Canetti and Krawczyk model is multi-party protocols (with the exception of the three-party case [HBN]). However, Katz and Yung [KY03] have proven secure a protocol compiler which works in a very similar way to an authenticator. Their compiler takes a protocol secure against a passive Bellare–Rogaway adversary (one which does not use Send queries) into one which is secure against an active adversary. It would be useful to understand the precise relationship between these related models.

5 Joining Forces

The formal methods approach to protocol analysis and the computational approach are both strong and active. In a sense their strengths and weaknesses are complementary. The formal methods approach uses an incomplete model of cryptography and lacks a transparent definition of security, but tool support gives strong assurance of analysis correctness and allows quick results to be obtained. The computational approach uses the normal definitions of cryptography, but the analysis results are slow to obtain and inaccessible to non-experts.

It is a natural goal to develop a complementary approach incorporating the strengths of both the approaches. One simple way to do this is to perform the Dolev-Yao style of analysis using the same adversary definition as used in the computational approach, but limited to deterministic actions. Surprisingly this has only recently been explored [CBHM04a]. This process allows a hand-proven computational proof to stand alongside an automatic Dolev-Yao style analysis with a simplified model of cryptography. Going beyond this, it would be helpful to specify and explore with tools the proof process used in the computational approach. This need not take the form of a complete automatic proof checker; even a modest analysis of a part of the proof could be very beneficial. Reductionist proofs typically work by plugging a problem instance into an adversary assumed to have an advantage in breaking the protocol of interest. This requires a *simulation* of the protocol in order to let the adversary operate normally. Correct specification of the simulation seems to be an area vulnerable to errors. Therefore a formal specification and exploration of this part of the proof could be a useful way to find errors in proofs.

An alternative direction is to provide cryptographically faithful abstractions of cryptography and use these to replace the existing black-box version of cryptography. Two large research efforts which provide the potential for this are Canetti's model for universal composability [Can01] and the reactive models of Pfitzmann *et al.* [PW01]. At present these models are still too new to have seen wide application. Recently Backes [Bac04] has illustrated the potential of this approach with a hand analysis of a well-known protocol. Another effort in this direction was initiated by Abadi and Rogaway [AR02] aimed at providing a formal notion of encryption that provides a sound replacement for the usual computational definitions. Lately this has been extended by others to incorporate active adversaries [MW04]. It will be interesting to see what new insights will be gained once software tools are incorporated into this line of work.

Acknowledgements

I am grateful to Juan González and Yvonne Hitchcock for their helpful comments and suggestions.

References

[ADR02] Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In *Advances in Cryptology - EUROCRYPT*

2002, pages 83–107. Springer-Verlag, 2002. Full version at `http://theory.lcs.mit.edu/~yevgen/ps/signcrypt.ps`.

[AFP04] Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval. Password-based authenticated key exchange in the three-party setting. Cryptology ePrint Archive, Report 2004/233, 2004. `http://eprint.iacr.org/`.

[AN94] Martín Abadi and Roger Needham. Prudent engineering practice for cryptographic protocols. In *IEEE Symposium on Research in Security and Privacy*, pages 122–136. IEEE Computer Society Press, 1994.

[AN95] Ross Anderson and Roger Needham. Robustness principles for public key protocols. In D. Coppersmith, editor, *Advances in Cryptology – Crypto '95*, pages 236–247. Springer-Verlag, 1995. Lecture Notes in Computer Science Volume 963.

[AR02] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, 2002.

[Bac04] Michael Backes. A cryptographically sounds Dolev–Yao style security proof on the Otway–Rees protocol. In *ESORICS 2004*, pages 89–108. Springer-Verlag, 2004.

[BCK98] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *30th ACM Symposium on Theory of Computing*, pages 419–428. ACM Press, 1998. Full version at `http://www-cse.ucsd.edu/users/mihir/papers/key-distribution.html`.

[BMP04] Colin Boyd, Wenbo Mao, and Kenny Paterson. Key agreement using statically keyed authenticators. In *Applied Cryptography and Network Security: Second International Conference*, pages 248–262. Springer-Verlag, 2004. Corrected version at `http://sky.fit.qut.edu.au/~boydc/papers/acns04-corrected.pdf`.

[BMV03] D. Basin, S. Mödersheim, and L. Viganò. An on-the-fly model-checker for security protocol analysis. In Einar Snekkenes and Dieter Gollmann, editors, *Proceedings of ESORICS'03*, LNCS 2808, pages 253–270. Springer-Verlag, 2003.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated key exchange secure against dictionary attacks. In B. Preneel, editor, *Advances in Cryptology – Eurocrypt 2000*, pages 139–155. Springer-Verlag, 2000. Lecture Notes in Computer Science Volume 1807.

[BR93] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology – Crypto '93*, pages 232–249. Springer-Verlag, 1993. Lecture Notes in Computer Science Volume 773. Full version at `http://www-cse.ucsd.edu/users/mihir`.

[BR95] Mihir Bellare and Phillip Rogaway. Provably secure session key distribution – the three party case. In *27th ACM Symposium on Theory of Computing*, pages 57–66. ACM Press, 1995.

[BS04] Michael Backes and Matthias Schunter. From absence of certain vulnerabilities towards security proofs. In *New Security Paradigms Workshop*, pages 67–74. ACM Press, 2004.

[Can01] Ran Canetti. Universally composable security: a new paradigm for cryptographic protocols (extended abstract). In IEEE, editor, *42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE Computer Society Press, 2001. Full version available at: `http://eprint.iacr.org/2000/067`.

[CBHM04a] Raymond Choo, Colin Boyd, Yvonne Hitchcock, and Greg Maitland. Complementing computational protocol analysis with formal specifications. In *Formal Aspects in Security and Trust*, Toulouse, 2004. To appear.

[CBHM04b] Raymond Choo, Colin Boyd, Yvonne Hitchcock, and Greg Maitland. On session identifiers in provably secure protocols: The bellare-rogaway three-party key distribution protocol revisited. In *Fourth Conference on Security in Communication Networks*. Springer-Verlag, 2004. To appear.

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature: Version 1.0. `http://www-users.cs.york.ac.uk/~jac/papers/drareview.ps.gz`, November 1997.

[CJ02] John Clark and Jeremy Jacob. Protocols are programs too: the meta-heuristic search for security protocols. *Information and Software Technology*, 43:891–904, 2002.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In B. Pfitzmann, editor, *Advances in Cryptology – Eurocrypt 2001*, pages 453–474. Springer-Verlag, 2001. Lecture Notes in Computer Science Volume 2045. `http://eprint.iacr.org/2001/040/`.

[DY83] D. Dolev and A. Yao. On the security of public-key protocols. *IEEE Transactions on Information Theory*, 29:198–208, 1983.

[EBP04] Olivier Chevassut Emmanuel Bresson and David Pointcheval. New security results on encrypted key exchange. In *International Workshop on Practice and Theory in Public Key Cryptography (PKC 2004)*, pages 145–158. Springer-Verlag, 2004. Also available at `http://www.di.ens.fr/~pointche/pub.php?reference=BrChPo04`.

[HBN] Yvonne Hitchcock, Colin Boyd, and Juan Manuel González Nieto. A password-based authenticator: Security proof and applications. In these proceedings.

[HC98] D. Harkins and D. Carrel. The internet key exchange (IKE). In *RFC 2409*. The Internet Society, 1998.

[HTN+03] Yvonne Hitchcock, Yiu Shing Terry Tin, Juan Manuel González Nieto, Colin Boyd, and Paul Montague. A password-based authenticator: Security proof and applications. In *Indocrypt 2003*, pages 388–401. Springer-Verlag, 2003. Full version at `http://sky.fit.qut.edu.au/~boydc/papers/password.ps.gz`.

[IEE04] IEEE. *P1363.2: Password-Based Public-Key Cryptography*, September 2004. `http://grouper.ieee.org/groups/1363/passwdPK/index.html`.

[KM04] Neal Koblitz and Alfred Menezes. Another look at "provable security". Cryptology ePrint Archive, Report 2004/152, 2004. `http://eprint.iacr.org/`.

[KY03] Jonathan Katz and Moti Yung. Scalable protocols for authenticated group key exchange. In *Advances in Cryptology – Crypto 2003*, pages 110–125. Springer-Verlag, 2003. Also available at `http://www.cs.umd.edu/~jkatz/papers/multi-auth.pdf`.

[Low96] Gavin Lowe. Breaking and fixing the Needham-Schroeder public key protocol using FDR. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 147–166. Springer-Verlag, 1996.

[Mac02] Philip MacKenzie. The PAK suite: Protocols for password-authenticated key exchange. Technical Report 2002-46, DIMACS, October 2002. `http://dimacs.rutgers.edu/TechnicalReports/abstracts/2002/2002-46.html`.

[Mea03] Catherine Meadows. Formal methods for cryptographic protocol analysis. *IEEE Journal on Selected Areas in Communications*, 21(1), 2003.

[MW04] Daniele Micciancio and Bogdan Warinschi. Soundness of formal encryption in the presence of active adversaries. In *First Theory of Cryptography Conference – TCC*, pages 133–151. Springer-Verlag, 2004.

[NS78] Roger Needham and Michael Schroeder. Using encryption for authentication in large network of computers. *Communications of the ACM*, 21:993–999, December 1978.

[PK00] Radia Perlman and Charlie Kaufman. Key exchange in IPSec: Analysis of IKE. *IEEE Internet Computing*, 4(6):50–56, November–December 2000.

[PW01] Birgit Pfitzmann and Michael Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *IEEE Symposium on Security and Privacy*, pages 184–200, 2001.

[TBN03] Yiu Shing Terry Tin, Colin Boyd, and Juan Manuel González Nieto. Provably secure mobile key exchange: Applying the Canetti-Krawczyk approach. In *Security and Privacy – ACISP 2003*, pages 166–179. Springer-Verlag, 2003.

[TVBN04] Yiu Shing Terry Tin, Harikrishna Vasanta, Colin Boyd, and Juan Manuel González Nieto. Protocols with security proofs for mobile applications. In *Security and Privacy – ACISP 2004*, pages 358–369. Springer-Verlag, 2004. Full version available at `http://sky.fit.qut.edu.au/~boydc/papers/ACISP04Full.pdf`.

[War03] B. Warinschi. A computational analysis of the needham-schroeder(-lowe) protocol. In *Proceedings of 16th Computer Science Foundation Workshop*, pages 248–262. ACM Press, 2003.

[WC01] Duncan S. Wong and Agnes H. Chan. Efficient and mutually authenticated key exchange for low power computing devices. In C. Boyd, editor, *Advances in Cryptology – Asiacrypt 2001*, pages 272–289. Springer-Verlag, 2001. Lecture Notes in Computer Science Volume 2248.

[Wie98] Michael J. Wiener. Performance comparison of public-key cryptosystems. *RSA Cryptobytes*, 4(1), 1998.